## CLAIMS

What is claimed is:

1. A method for managing identification in a data communications network, the method comprising:

receiving a user-controlled secure storage device;

enrolling said user with an authority network site, said enrolling comprising

providing information requested by said authority network site;

receiving user data in response to said enrolling;

storing said user data in said user-controlled secure storage device;

enabling said user-controlled secure storage device to release said user data; and

using said user data at a service provider network site to obtain a service.

2. A method for managing identification in a data communications network, the method comprising:

receiving a user-controlled secure storage device;

enrolling said user with an authority network site, said enrolling comprising

providing information requested by said authority network site;

receiving user data in response to said enrolling, said user data comprising a first portion and a second portion, said first portion comprising a cryptogram computed based on said second portion;

storing said user data in said user-controlled secure storage device;

enabling said user-controlled secure storage device to release said user data; and

using said user data at a service provider network site to obtain a service.

3. A method for managing identification in a data communications network, the method comprising:

presenting an identity credential request and data to be stored to a federated identity server via a client host;

receiving an identity credential in response to said identity credential request, said identity credential comprising a randomized ID and an identification authority ID, said federated identity server capable of verifying the truthfulness, accuracy and completeness of said data to be stored;

presenting a service request and said identity credential to said service portal, said service portal configured to issue an authentication request to said federated identity server;

receiving a logon credential in response to said service request, said login credential comprising an indication of the client host used by the user;

using said logon credential to obtain a service from a service provider accessible via said service portal.

4. A program storage device readable by a machine, embodying a program of instructions executable by the machine to perform a method for managing identification in a data communications network, the method comprising:

receiving a user-controlled secure storage device;

enrolling said user with an authority network site, said enrolling comprising

providing information requested by said authority network site;

receiving user data in response to said enrolling;

storing said user data in said user-controlled secure storage device;

enabling said user-controlled secure storage device to release said user data; and

using said user data at a service provider network site to obtain a service.

5. A program storage device readable by a machine, embodying a program of instructions executable by the machine to perform a method for managing identification in a data communications network, the method comprising:

receiving a user-controlled secure storage device;

enrolling said user with an authority network site, said enrolling comprising

providing information requested by said authority network site;

receiving user data in response to said enrolling, said user data comprising a first portion and a second portion, said first portion comprising a cryptogram computed based on said second portion;

storing said user data in said user-controlled secure storage device;

enabling said user-controlled secure storage device to release said user data; and

using said user data at a service provider network site to obtain a service.

6. A program storage device readable by a machine, embodying a program of instructions executable by the machine to perform a method for managing identification in a data communications network, the method comprising:

presenting an identity credential request and data to be stored to a federated identity server via a client host;

receiving an identity credential in response to said identity credential request, said identity credential comprising a randomized ID and an identification authority ID, said federated identity server capable of verifying the truthfulness, accuracy and completeness of said data to be stored;

presenting a service request and said identity credential to said service portal, said service portal configured to issue an authentication request to said federated identity server;

receiving a logon credential in response to said service request, said login credential comprising an indication of the client host used by the user;

using said logon credential to obtain a service from a service provider accessible via said service portal.

7. An apparatus for managing identification in a data communications network, the apparatus comprising:

means for receiving a user-controlled secure storage device;

means for enrolling said user with an authority network site, said enrolling comprising providing information requested by said authority network site;

means for receiving user data in response to said enrolling;

means for storing said user data in said user-controlled secure storage device;

means for enabling said user-controlled secure storage device to release said user data; and

means for using said user data at a service provider network site to obtain a service.

8. An apparatus for managing identification in a data communications network, the apparatus comprising:

means for receiving a user-controlled secure storage device;

means for enrolling said user with an authority network site, said enrolling comprising providing information requested by said authority network site;

means for receiving user data in response to said enrolling, said user data comprising a first portion and a second portion, said first portion comprising a cryptogram computed based on said second portion;

means for storing said user data in said user-controlled secure storage device;

means for enabling said user-controlled secure storage device to release said user data; and

means for using said user data at a service provider network site to obtain a service.

9. An apparatus for managing identification in a data communications network, the apparatus comprising:

means for presenting an identity credential request and data to be stored to a federated identity server via a client host;

means for receiving an identity credential in response to said identity credential request, said identity credential comprising a randomized ID and an identification authority ID, said federated identity server capable of verifying the truthfulness, accuracy and completeness of said data to be stored;

means for presenting a service request and said identity credential to said service portal, said service portal configured to issue an authentication request to said federated identity server;

receiving a logon credential in response to said service request, said login credential comprising an indication of the client host used by the user;

using said logon credential to obtain a service from a service provider accessible via said service portal.

10. A method for protecting privacy on a data communications network, the method comprising:

receiving a user identifier and specific user data associated with said user identifier, said specific user data comprising data about a network user;

creating generalized user data based on said specific user data;

associating said generalized user data with said user identifier; and

returning said user identifier and said generalized user data.

11. A method for protecting privacy on a data communications network, the method comprising:

presenting a user identifier and specific user data associated with said user identifier to an authority, said specific user data comprising data about a network user;

receiving generalized user data based on said specific user data in response to said presenting; and

using said generalized user data to obtain a service on said data communications network.

12. A method for protecting privacy on a data communications network, the method comprising:

storing user logon information for at least one service provider server on a user-controlled secure device, said at least one service provider server comprising at least one network server that is capable of providing a service to a user; and

logging on to said device, said logging on providing access to said at least one service provider server.

13. An apparatus for protecting privacy on a data communications network, the apparatus comprising:

means for receiving a user identifier and specific user data associated with said user identifier, said specific user data comprising data about a network user;

means for creating generalized user data based on said specific user data;

means for associating said generalized user data with said user identifier; and

means for returning said user identifier and said generalized user data.

14. An apparatus for protecting privacy on a data communications network, the apparatus comprising:

means for presenting a user identifier and specific user data associated with said user identifier to an authority, said specific user data comprising data about a network user;

means for receiving generalized user data based on said specific user data in response to said presenting; and

means for using said generalized user data to obtain a service on said data communications network.

15. An apparatus for protecting privacy on a data communications network, the apparatus comprising:

means for storing user logon information for at least one service provider server on a user-controlled secure device, said at least one service provider server comprising at least one network server that is capable of providing a service to a user; and

means for logging on to said device, said logging on providing access to said at least one service provider server.

16. An apparatus for protecting privacy on a data communications network, the apparatus comprising:

receiving a user identifier and specific user data associated with said user identifier, said specific user data comprising data about a network user;

creating generalized user data based on said specific user data;

associating said generalized user data with said user identifier; and

returning said user identifier and said generalized user data.

17. An apparatus for protecting privacy on a data communications network, the apparatus comprising:

presenting a user identifier and specific user data associated with said user identifier to an authority, said specific user data comprising data about a network user;

receiving generalized user data based on said specific user data in response to said presenting; and

using said generalized user data to obtain a service on said data communications network.

18. An apparatus for protecting privacy on a data communications network, the apparatus comprising:

means for storing user logon information for at least one service provider server on a user-controlled secure device, said at least one service provider server comprising at least one network server that is capable of providing a service to a user; and

means for logging on to said device, said logging on providing access to said at least one service provider server.

19. A memory for storing data for access by an application program being executed on a data processing system, comprising:

a data structure stored in said memory, said data structure including a bit-mapped field associated with a data communications network user, the value of each bit in said field determined by whether said user is a member of a group associated with said bit, the mapping for between bits in said field and membership in a group maintained by an aggregation authority.